**PCT** WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G06F 12/14

A1

(11) Internationale Veröffentlichungsnummer: **WO 98/16883**

(43) Internationales Veröffentlichungsdatum: 23. April 1998 (23.04.98)

(21) Internationales Aktenzeichen: PCT/DE97/02070

(22) Internationales Anmeldedatum: 15. September 1997 (15.09.97)

(30) Prioritätsdaten:
196 42 560.3 15. Oktober 1996 (15.10.96) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: PFAB, Stefan [DE/DE]; Wettersteinstrasse 2, D–82049 Großhesselohe (DE).

(81) Bestimmungsstaaten: BR, CN, JP, KR, MX, RU, UA, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

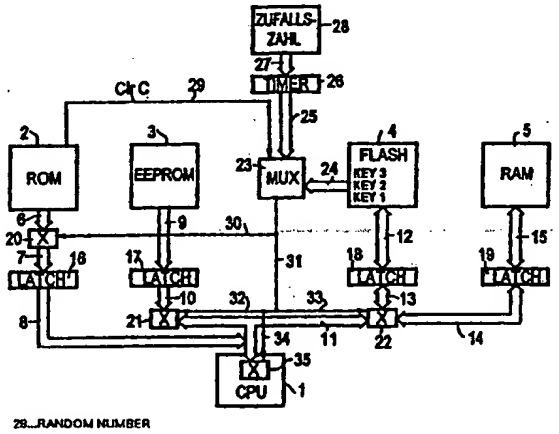
Veröffentlicht
*Mit internationalem Recherchenbericht.*
*Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.*

(54) Title: ELECTRONIC DATA PROCESSING CIRCUIT

(54) Bezeichnung: ELEKTRONISCHE DATENVERARBEITUNGSSCHALTUNG

(57) Abstract

The invention concerns an electronic data processing circuit having an operating module (1, 101), such as for example a microprocessor, with at least one data memory (2, 3, 4, 5, 102, 103, 104, 105) and with a data bus (106) extending between a data memory (2, 3, 4, 5, 102, 103, 104, 105) and the operating module (1, 101). With electronic data processing circuits of the type in question the memory frequently contains information to which access should be limited as far as possible. Therefore it is necessary to take security measures to guard against manipulation of the electronic data processing circuit. Consequently the object of the invention is to produce an electronic data processing circuit of the type in question which affords better protection against undesired alterations. According to the invention, this object is achieved by an electronic data processing circuit of the type in question in which at least one coding module (20, 21, 22, 35, 107) is provided in the region between the data memory (2, 3, 4, 5, 102, 103, 104, 105) and the data bus and/or in the region between the operating module (1, 101) and the data bus. The coding module (20, 21, 22, 35, 107) is designed such that data traffic between the operating module (1, 101) and the data bus or between the data memory (2, 3, 4, 5, 102, 103, 104, 105) and the data bus (106) can be coded and/or decoded.



(57) **Zusammenfassung**

Die Erfindung betrifft eine elektronische Datenverarbeitungschaltung mit einer Betriebsbaugruppe (1, 101) wie beispielsweise einem Mikroprozessor, mit wenigstens einem Datenspeicher (2, 3, 4, 5, 102, 103, 104, 105) und mit einem sich zwischen Datenspeicher (2, 3, 4, 5, 102, 103, 104, 105) und Betriebsbaugruppe (1, 101) erstreckendem Datenbus (106). Bei den gattungsgemäßen elektronischen Datenverarbeitungsschaltungen enthält der Speicher häufig Informationen, auf die möglichst nicht zugegriffen werden soll. Deshalb ist es notwendig, Sicherheitsmaßnahmen gegen Manipulationen der elektronischen Datenverarbeitungsschaltung zu treffen. Es ist daher Aufgabe der Erfindung, eine gattungsgemäße elektronische Datenverarbeitungsschaltung bereitzustellen, die einen verbesserten Schutz gegen unerwünschte Veränderungen aufweist. Diese Aufgabe wird gemäß der Erfindung durch eine gattungsgemäße elektronische Datenverarbeitungsschaltung gelöst, bei der im Bereich zwischen Datenspeicher (2, 3, 4, 5, 102, 103, 104, 105) und Datenbus und/oder im Bereich zwischen Betriebsbaugruppe (1, 101) und Datenbus wenigstens eine Verschlüsselungsbaugruppe (20, 21, 22, 35, 107) vorgesehen ist, wobei die Verschlüsselungsbaugruppe (20, 21, 22, 35, 107) so ausgebildet ist, daß Datenverkehr zwischen Betriebsbaugruppe (1, 101) und Datenbus bzw. zwischen Datenspeicher (2, 3, 4, 5, 102, 103, 104, 105) und Datenbus (106) verschlüsselbar und/oder entschlüsselbar ist.



BNSDOCID: <WO 9816883A1 I >

# Elektronische Datenverarbeitungsschaltung

## Beschreibung

Die Erfindung betrifft eine elektronische Datenverarbeitungsschaltung mit einer Betriebsbaugruppe wie beispielsweise einem Mikroprozessor, mit wenigstens einem Datenspeicher und mit einem sich zwischen Datenspeicher und Betriebsbaugruppe erstreckendem Datenbus.

Die gattungsgemäßen elektronischen Datenverarbeitungsschaltungen werden häufig bei sicherheitskritischen Anwendungen eingesetzt. Dabei werden im Datenspeicher vertrauliche Daten, Geldwerte und Zugangsberechtigungen abgelegt, die von der Betriebsbaugruppe beispielsweise auf eine externe Anforderung hin verarbeitet werden.

Da der Speicher Informationen enthält, auf die möglichst nicht zugegriffen werden soll, ist es notwendig, Sicherheitsmaßnahmen gegen Manipulationen der elektronischen Datenverarbeitungsschaltung zu treffen.

Wenn eine gattungsgemäße elektronische Datenverarbeitungsschaltung als integrierter Schaltkreis ausgeführt ist, kann diese mit verschiedenen Passivierungsschichten abgedeckt werden. Dabei können die Passivierungsschichten so angelegt sein, daß eine Entfernung einer Passivierungsschicht die Zerstörung des Datenspeichers zur Folge hat. Weiterhin kann man den Datenspeicher in tieferliegenden Schichten des integrierten Schaltkreises vergraben, so daß der Zugriff auf ihn erschwert wird.

Eine weitere Möglichkeit, eine elektronische Datenverarbeitungsschaltung gegen unerwünschte Manipulationen zu schützen, besteht in der Verwendung von Sensoren, die Betriebsbedingungen der elektronischen Datenverarbeitungsschaltung abtasten. Sobald ein von einem Sensor abgetasteter

Wert außerhalb eines normalen Wertes liegt, werden entsprechende Sicherungsmaßnahmen ausgelöst, die zu einer Inaktivierung der elektronischen Datenverarbeitungsschaltung oder auch zu einem Löschen des Datenspeichers führen.

Weiterhin gibt es auch Software-Sensoren, die den Betrieb der Betriebsbaugruppe auf verbotene Befehle hin oder auf Zugriffe auf Adressbereiche hin überwachen, die für einen bestimmungsgemäßen Betrieb gesperrt sind. Außerdem kann die Zugangssequenz auf ihre Richtigkeit hin überwacht werden.

Schließlich ist es noch bekannt, in einem besonderen Herstellungsmodus erlaubte Speicherzugriffe der Betriebsbaugruppe auf den Datenspeicher durch besondere Hardware-Vorrichtungen wie beispielsweise auftrennbar ausgestaltete Verbindungsbahnen einzuschränken.

Trotz der bevorstehend ausgeführten Sicherheitsmaßnahmen kommt es dennoch gelegentlich zu unerwünschten Manipulationen an den gattungsgemäßen elektronischen Datenverarbeitungsschaltungen.

Es ist daher Aufgabe der Erfindung, eine gattungsgemäße elektronische Datenverarbeitungsschaltung bereitzustellen, die einen verbesserten Schutz gegen unerwünschte Veränderungen aufweist.

Diese Aufgabe wird gemäß der Erfindung durch eine gattungsgemäße elektronische Datenverarbeitungsschaltung gelöst, bei der weiterhin im Bereich zwischen Datenspeicher und Datenbus und/oder im Bereich zwischen Betriebsbaugruppe und Datenbus wenigstens eine Verschlüsselungsbaugruppe vorgesehen ist, wobei die Verschlüsselungsbaugruppe so ausgebildet ist, daß Datenverkehr zwischen Betriebsbaugruppe und Datenbus bzw. zwischen Datenspeicher und Datenbus verschlüsselbar und/oder entschlüsselbar ist.

Die Erfindung beruht auf der erfindungswesentlichen Erkenntnis, daß sich durch neue technische Verfahren die Manipulierbarkeit gerade von als integrierte Schaltkreise ausgeführte elektronische Datenverarbeitungsschaltungen erleichtert hat. So ist aus der Sicht eines Manipulierers eine elektronische Datenverarbeitungsschaltung in einem integrierten Schaltkreis nicht mehr nur als Chip in seiner Gesamtheit zu sehen, sondern als ein aus einzelnen Komponenten auf einem Siliziumträger bestehendes System, bei dem auf die Komponenten separat zugegriffen werden kann.

Demzufolge gibt es die Möglichkeit, durch Beobachtung des Datenverkehrs auf dem Datenbus oder durch Auslesen des Datenspeichers Rückschlüsse auf die im Datenspeicher gespeicherten Informationen zu ziehen, so daß eine Manipulation erleichtert wird.

Gemäß einer weiteren erfindungswesentlichen Erkenntnis lassen sich viele Manipulationen an den gattungsgemäßen elektronischen Datenverarbeitungsschaltungen darauf zurückführen, daß es gelungen ist, den Datenverkehr auf dem Datenbus "abzuhören", so daß der Programmablauf in der Betriebsbaugruppe beobachtet und unerwünschterweise verstanden werden kann.

Gemäß der Erfindung wird vorgeschlagen, die Daten in der elektronischen Datenverarbeitungsschaltung verschlüsselt zu transportieren, wobei zwischen Datenbus und Datenspeicher bzw. Betriebsbaugruppe und Datenbus Einrichtungen vorgesehen sind, um den auf dem Datenbus transportierten Datenverkehr zu verschlüsseln und zu entschlüsseln. Die derartigen Einrichtungen werden nachfolgend mit "Verschlüsselungsbaugruppe" bezeichnet, wobei diese Bezeichnung ausdrücklich nicht auf Einrichtungen beschränkt ist, die lediglich eine Verschlüsselung ausführen. Gemäß dem Grundgedanken der Erfindung sind mit dieser Bezeichnung auch Einrichtungen gemeint, die sowohl eine Verschlüsselung als auch eine

Entschlüsselung bzw. nur eine dieser beiden Operationen ausführen.

Durch die erfindungsgemäße Ausgestaltung der elektronischen Datenverarbeitungsschaltung ist gewährleistet, daß selbst bei einem erfolgreichen Nachverfolgen des Datenverkehrs auf dem Datenbus nicht direkt auf die im Datenspeicher gespeicherten Daten geschlossen werden kann. Weiterhin ist es nicht ohne weiteres möglich, aus den beim Nachverfolgen des Datenverkehrs auf dem Datenbus gewonnenen Informationen auf den Programmablauf zurückzuschließen. Selbst bei einem erfolgreichen Auslesen der im Datenspeicher gespeicherten Daten kann nämlich nicht ohne weiteres auf deren Bedeutung zurückgeschlossen werden, da diese für einen unbefangenen Beobachter keinen Sinn ergeben.

Dabei ist es gemäß der Erfindung besonders vorteilhaft, daß die Verschlüsselung und Entschlüsselung gemäß der Erfindung über den gesamten Chip verteilt bzw. disloziert erfolgt, weil für eine erfolgreiche Manipulation eine gleichzeitige Beobachtung von mehreren Stellen der elektronischen Datenverarbeitungsschaltung notwendig wäre, was technisch nur schwer durchzuführen ist.

Dabei ist bei einem mit Latch-Zwischenspeicher zur Zwischenspeicherung von Zugriffen auf den Datenspeicher versehenen elektronischen Datenverarbeitungsschaltungen wesentlich, daß die Verschlüsselungsbaugruppe so angeordnet wird, daß der Inhalt des Latch-Zwischenspeichers stets verschlüsselt ist. Der Inhalt der Latches kann nämlich relativ leicht beobachtet werden, so daß deren Inhalt im Betrieb der erfindungsgemäßen Datenverarbeitungsschaltung sicherheitshalber verschlüsselt vorliegen muß.

Die Verschlüsselung und Entschlüsselung kann sich gemäß der Erfindung bis in eine CPU einer erfindungsgemäßen Datenverarbeitungsschaltung hinein erstrecken. Darüber hinaus

kann die Verschlüsselung und die Entschlüsselung auch voneinander unabhängig in mehreren Verschlüsselungsbaugruppen erfolgen. Gemäß der Erfindung werden aber auch Lösungen umfaßt, bei der nur eine einzige Verschlüsselungsbaugruppe vorgesehen ist.

Schließlich ergibt sich noch ein Vorteil bei Datenverarbeitungsschaltungen, die in einer Multitasking-Verarbeitung verschiedene Applikationen simultan verarbeiten. Dann können durch geeignete Verschlüsselung verschiedenen Applikationen bzw. Tasks verschiedene Datenspeicher zugeordnet werden, wobei für jede Task ein unterschiedlicher Schlüssel vereinbart wird. Dadurch kann eine Task nicht auf Daten der anderen Task zugreifen.

Zusammenfassend läßt sich daher feststellen, daß es gemäß der Erfindung nun nicht mehr genügt, die Datenverarbeitungsschaltung nur physikalisch zu untersuchen. Zusätzlich muß nun insbesondere unter gleichzeitiger Beobachtung mehrerer Komponenten auch der in der Verschlüsselungsbaugruppe bzw. in den Verschlüsselungsbaugruppen gespeicherte Schlüssel und gegebenenfalls die Aktivierung dieses Schlüssels erkannt werden.

In Ausbildung der Erfindung ist die Verschlüsselungsbaugruppe so ausgebildet, daß Datenverkehr auf dem Datenbus mittels eines Verschlüsselungs-Algorithmus verschlüsselbar ist. Eine derartig ausgebildete Verschlüsselungsbaugruppe bringt den Vorteil mit sich, bei einer Massenfertigung besonders kostengünstig herstellbar zu sein. Jedoch dauert eine Verschlüsselung mit einem Algorithmus sehr lang, da dadurch umfangreiche Berechnungen in der Betriebsbaugruppe notwendig werden. Ein Echtzeit-Betrieb dieser erfindungsgemäßen Datenverarbeitungsschaltung ist daher derzeit noch nicht möglich.

In weiterer Ausgestaltung der Erfindung ist die Verschlüsselungsbaugruppe so ausgebildet, daß Datenverkehr auf dem Datenbus mittels Hardware-Verschlüsselung verschlüsselbar ist. Gerade bei Hardware-Verschlüsselung ist ein Betrieb der erfindungsgemäßen Datenverarbeitungsschaltungen in Echtzeit bereits auf sehr einfache Weise zu verwirklichen, und zwar sowohl bei Lese- als auch bei Schreibzugriff auf den Datenspeicher.

Eine Hardware-Verschlüsselung kann gemäß der Erfindung mit einer Verschlüsselungsbaugruppe erfolgen, die so ausgebildet ist, daß die Wertigkeiten einzelner Bit des Datenverkehrs selektiv änderbar ist. Dann erscheinen Bits, die im Speicher beispielsweise als "LOW" abgelegt sind, im Datenverkehr auf dem Datenbus als "HIGH". Dies kann zum Beispiel mit einer Verschlüsselungsbaugruppe erfolgen, die wenigstens ein EXOR-Glied aufweist.

In weiterer Ausgestaltung der Erfindung kann die Verschlüsselungsbaugruppe so ausgebildet sein, daß die Anschlußreihenfolge von Datenleitungen des Datenbus selektiv änderbar ist. Dies äußert sich nach außen hin so, als ob einzelne Bitleitungen des Datenbus vertauscht wären.

Schließlich kann die Hardware-Verschlüsselung bei der erfindungsgemäßen Datenverarbeitungsschaltung auch durch eine Verschlüsselungsbaugruppe ausgeführt werden, die so ausgebildet ist, daß der Datenverkehr zwischen Datenbus und Betriebsbaugruppe und/oder zwischen Datenbus und Datenspeicher wenigstens teilweise selektiv verzögerbar ist. Dadurch wird auf dem Datenbus ein Datenverkehr vorgetäuscht, der keinen Bezug zu dem momentanen Betriebszustand der erfindungsgemäßen elektronischen Datenverarbeitungsschaltung hat.

Dabei besteht ein wesentliches Merkmal der erfindungsgemäßen Datenverarbeitungsschaltung darin, daß die

Verschlüsselungsbaugruppe so ausgebildet ist, daß die Verschlüsselung selektiv arbeitet. Dies bedeutet nicht nur, daß eine Verschlüsselung wahlweise erfolgen oder unterbleiben kann. Darüber hinaus umfaßt dies gemäß der Erfindung auch, daß zwischen verschiedenen Schlüsseln zum Verschlüsseln des Datenverkehrs gewechselt werden kann. In diesem Fall bekommt der Einsatz der erfindungsgemäßen Verschlüsselungsbaugruppe ein dynamisches Verhalten.

Gerade bei der erfindungsgemäßen Datenverarbeitungsschaltung mit wechselnden Schlüsseln ist vorgesehen, daß Datenverarbeitungsschaltungen eines Fertigungsloses jeweils unterschiedliche und individuelle Schlüssel bekommen. Dadurch ist gewährleistet, daß selbst bei Kenntnis des Schlüssels einer Datenverarbeitungsschaltung noch nicht auf die Schlüssel anderer Datenverarbeitungsschaltungen geschlossen werden kann.

In Ausgestaltung des Grundgedankens der Erfindung weist die Verschlüsselungsbaugruppe wenigstens einen Eingang zur Eingabe wenigstens eines Schlüssels auf. Dieser Eingang in die Verschlüsselungsbaugruppe kann jedoch auch dazu verwendet werden, zwischen bestimmten, in der Verschlüsselungsbaugruppe selbst gespeicherten Schlüsseln und sogar zwischen den in der Verschlüsselungsbaugruppe angewendeten Verschlüsselungsverfahren umzuschalten. Es ist auch ganz einfach möglich, ein einziges Verschlüsselungsverfahren zu aktivieren bzw. zu deaktivieren. Abweichend davon kann über den Eingang auch ein außerhalb der Verschlüsselungsbaugruppe abgespeicherter Schlüssel eingegeben werden. Dazu wird der Schlüssel vorteilhafterweise in einer FLASH-Zelle oder in einer EEPROM-Zelle abgelegt. Die vorstehenden Zellen gelten als relativ sicher, weil die Informationen auf einem Floating-Gate mit nur "wenigen" Elektronen gespeichert sind. Die meisten Versuche, deren Inhalt auszulesen, zerstören die gespeicherte Information. Von daher ergibt sich gemäß dieser Ausgestaltung der Erfindung eine besonders sichere Verschlüsselung des

Datenverkehrs. Weiterhin haben alle FLASH-Zellen den Vorteil der Programmierbarkeit. So können auf einfache Weise bei der Auslieferung der erfindungsgemäßen Datenverarbeitungsschaltung in jede Schaltung individuelle Schlüssel einprogrammiert und für weitere Veränderungen gesperrt werden.

Eine weitere Verbesserung der Sicherheit ergibt sich dann, wenn der Schlüssel in einer vergrabenen Struktur eines integrierten Bausteins abgelegt ist, wobei der integrierte Baustein vorteilhafterweise auch die Datenverarbeitungsschaltung aufnimmt. Vergrabene Strukturen bieten den Vorteil, daß sie dezentral an verschiedenen Stellen des integrierten Bausteins ausgeführt werden können. Dies erhöht die Sicherheit beträchtlich, da es sehr schwierig ist, verschiedene Stellen einer in einen integrierten Baustein aufgenommenen Datenverarbeitungsschaltung gleichzeitig zu beobachten. Darüber hinaus können auch Sensoren vorgesehen sein, die Manipulationen des Orts, an dem der Schlüssel abgelegt ist, abtasten und die erfindungsgemäße Datenverarbeitungsschaltung für diesen Fall deaktivieren oder sonstwie unbrauchbar machen.

Alternativ zu den bei der Herstellung der erfindungsgemäßen Datenverarbeitungsschaltung abgespeicherten Schlüsseln kann jedoch auch ein Zufallsgenerator vorgesehen sein, mit dem ein Schlüssel zufällig auswählbar ist.

Gemäß einer besonders vorteilhaften Ausgestaltung der Erfindung wird die Auswahl des in der Verschlüsselungsbaugruppe verwendeten Schlüssels von der Betriebsbaugruppe insbesondere während des Programmablaufs durchgeführt. Dazu ist die Datenverarbeitungsschaltung gemäß der Erfindung so ausgebildet, daß bei Ausführung vorbestimmter Operationen durch die Betriebsbaugruppe ein Schlüssel an die Verschlüsselungsbaugruppe eingebbar ist. Da der Programmcode der Betriebsbaugruppe eventuell bekannt sein

kann, erfolgt die Schlüsselauswahl vorteilhafterweise versteckt im normalen Programmcode. So könnte die Betriebsbaugruppe beispielsweise derart ausgebildet sein, daß bei Ausführen eines unverfänglichen Befehls wie beispielsweise CLR C ("CLEAR CARRY") der Schlüssel der Verschlüsselungs-baugruppe bzw. Verschlüsselungsbaugruppen gewechselt wird.

Darüber hinaus kann auch eine Zeitmessvorrichtung vorgesehen sein, die einen Wechsel des Schlüssels überwacht, und einen solchen Wechsel auslöst, wenn der Schlüssel nicht oft genug gewechselt wird.

Schließlich ist hinsichtlich der in den Verschlüsselungsbaugruppen verwendeten Schlüssel vorgesehen, daß die Schlüssel durch die Betriebsbaugruppe bzw. die CPU erzeugt werden. Dies erfolgt beispielsweise durch Ableiten eines Schlüssels mit einem Umsetzungsverfahren aus einer durch die CPU generierten Adresse. Der Vorteil dieses Verfahrens besteht darin, daß sich der Schlüssel ständig - also mit jeder Adresse - ändert. Durch die Auswahl verschiedener Umsetzungsverfahren kann der Programmierer der Betriebsbaugruppe auf die Verschlüsselung Einfluß nehmen.

Zusammenfassend ist zu sagen, daß der Datenverkehr in der erfindungsgemäßen Datenverarbeitungsschaltung von einem Manipulierer nur dann verstanden werden kann, wenn der jeweils in der Verschlüsselungsbaugruppe verwendete Schlüssel bekannt ist. Auch die im Datenspeicher abgelegten Daten können nur unter Kenntnis des zum Datenspeicher zugehörigen Schlüssels verstanden werden. Dies erhöht die Sicherheit gegen Manipulationen beträchtlich.

Selbstverständlich muß ein Programmierer, der die Betriebs-baugruppe der Datenverarbeitungsschaltung programmiert, eine vertrauliche Liste führen, welche zum Schlüssel zugehörigen

Daten er in welchen Adressen des Datenspeichers bzw. der Datenverarbeitungsschaltung abgelegt hat. Je nach Art des Schlüssels kann der Programmierer auch gewisse zu erfüllende Vorbedingungen vorsehen, die sich beispielsweise dadurch äußern, daß immer Werte-Paare gelesen werden müssen.

In einer besonders vorteilhaften Ausgestaltung der elektronischen Datenverarbeitungsschaltung sind im Bereich mindestens einer die Betriebsbaugruppe und wenigstens einen Datenspeicher verbindenden Datenleitung des Datenbus wenigstens zwei Verschlüsselungsbaugruppen vorgesehen, die so ausgebildet sind, daß eine vollständige Verschlüsselung bzw. Entschlüsselung erst durch das Zusammenwirken der beiden Verschlüsselungsbaugruppen ausführbar ist. Vorteilhafterweise sind die beiden Verschlüsselungsbaugruppen dabei an verschiedenen Orten der elektronischen Datenverarbeitungsschaltung angeordnet. Durch diese Ausgestaltung ist gewährleistet, daß eine Verschlüsselung des Datenverkehrs an zwei verschiedenen Orten erfolgt. Ein typischer Manipulierer wird möglicherweise nur eine Verschlüsselung an einem einzigen Ort, nämlich bei einer einzigen Verschlüsselungsbaugruppe nachvollziehen und beim Anwenden der Verschlüsselung trotzdem zu keinem brauchbaren Ergebnis kommen. Gerade bei einer Ausführung mit zwei Verschlüsselungsbaugruppen, die an verschiedenen Orten untergebracht sind, ist es nämlich besonders schwierig, eine Verschlüsselung nachzuvollziehen, da zwei verschiedene Orte einer Mikrostruktur nur auf besonders schwierige Weise gleichzeitig beobachtet werden können. Die so ausgeführten Verschlüsselungsbaugruppen können beispielsweise dergestalt ausgeführt sein, daß eine Verschlüsselungsbaugruppe an einem Ort die unteren vier Bits eines Datenbus verschlüsselt bzw. entschlüsselt, während die andere Verschlüsselungsbaugruppe die übrigen Bits des Datenbus verschlüsselt bzw. entschlüsselt.

Ein weiterer Vorteil des erfindungsgemäßen Verfahrens ergibt sich bei denjenigen gattungsgemäßen Datenverarbeitungs-

schaltungen, bei denen man aus Sicherheitsgründen erreichen möchte, daß nicht alle Komponenten der Datenverarbeitungsschaltung miteinander kommunizieren können. Dann kann durch geeignete Ausgestaltung des Schlüssels beispielsweise mit einer definierten Anzahl von Verschlüsselungs-Einheiten nur bei den dafür vorgesehenen Verbindungswegen des Datenbus kommuniziert werden. Alle anderen Verbindungen mit nicht geeigneten Verschlüsselungen können nicht richtig funktionieren.

Die Erfindung ist in der Zeichnung anhand zweier einfacher sowie eines komplexeren Ausführungsbeispiels in drei Figuren näher veranschaulicht. Es zeigen:

Figur 1 zeigt eine erfindungsgemäße elektronische Datenverarbeitungsschaltung mit nur einer einzigen Verschlüsselungseinrichtung in der CPU,

Figur 2 zeigt eine Variante der elektronischen Datenverarbeitungsschaltung aus Figur 1, und

Figur 3 zeigt eine weitere erfindungsgemäße elektronische Datenverarbeitungsschaltung mit Verschlüsselungseinrichtungen in der CPU sowie im Bereich der Datenspeicher.

Figur 1 zeigt eine erfindungsgemäße Datenverarbeitungsschaltung, die eine CPU 101 als Betriebsbaugruppe sowie mehrere Datenspeicher aufweist. Im Einzelnen sind dies ein ROM 102, ein EEPROM 103, ein FLASH-Speicher 104 sowie ein RAM 105. Die Datenspeicher 102, 103, 104, 105 und die CPU 101 sind über einen Datenbus 106 miteinander verbunden.

In der CPU 101 ist eine Verschlüsselungsbaugruppe 107 vorgesehen, die den Datenverkehr zwischen CPU 1 und den Datenspeichern 102, 103, 104 sowie 105 verschlüsselt bzw. entschlüsselt. Hier sei noch einmal darauf hingewiesen, daß

die derartige Einrichtung nachfolgend mit "Verschlüsselungsbaugruppe" bezeichnet wird, obwohl sie ausdrücklich nicht auf eine Einrichtung beschränkt ist, die lediglich eine Verschlüsselung ausführt. Gemäß dem Grundgedanken der Erfindung ist mit dieser Bezeichnung auch eine Einrichtung gemeint, die sowohl eine Verschlüsselung als auch eine Entschlüsselung bzw. nur eine dieser beiden Operationen ausführt. Die Ver- bzw. Entschlüsselung kann dabei durch eine geeignete Verzögerung, durch ein Vertauschen von einzelnen Bitleitungen des Datenbus oder durch ein Verändern der Wertigkeiten einzelner Datenbits erfolgen. Auch eine Software-Verschlüsselung kann ausgeführt werden.

Weiterhin hat die erfindungsgemäße Datenverarbeitungsschaltung einen Multiplexer 108, der über eine Datenleitung 109 mit dem FLASH-Speicher 104 in Verbindung steht. Der Multiplexer 108 steht über eine Datenleitung 110 mit einem Timer 111 in Verbindung, dem über eine Datenleitung 112 von einem Zufallsgenerator 113 eine Zufallszahl zuführbar ist. Der Multiplexer 108 weist auch eine Ansteuerleitung 114 auf, über die er mit dem ROM 102 in Verbindung steht. Schließlich ist noch eine RESET-Leitung 115 zum Multiplexer 108 vorgesehen, über die der Multiplexer 108 bei einem Reset der Datenverarbeitungsschaltung auf einen Grundzustand rücksetzbar ist. Der Ausgang des Multiplexers 108 steht über eine Ansteuerleitung 116 mit der Verschlüsselungsbaugruppe 107 in Verbindung, wobei die Verschlüsselungsbaugruppe 107 auf ein Ausgangssignal des Multiplexers 108 hin mit einem neuen Schlüssel versorgt wird. Erfindungsgemäß ist auch vorgesehen, daß in der Verschlüsselungsbaugruppe 107 auf ein Ausgangssignal des Multiplexers 108 über die Ansteuerleitung 116 hin das in der Verschlüsselungsbaugruppe 107 verwendete Verschlüsselungsverfahren umgeschaltet wird.

Im Betrieb verhält sich die erfindungsgemäße elektronische Datenverarbeitungsschaltung wie folgt. Beim Programmstart (RESET) wird auf ein Signal auf der RESET-Leitung 115 im

Multiplexer ein Start-Schlüssel eingestellt. Daraufhin wird der Datenverkehr zwischen Datenbus 106 und CPU 101 in der Verschlüsselungsbaugruppe 107 verschlüsselt bzw. entschlüsselt, wobei bei jedem Durchgang von Daten durch die Verschlüsselungsbaugruppe 107 eine entsprechende Operation entsprechend der Datenflußrichtung ausgeführt wird. Bei jeder Ausführung des Befehls "CLR C" übermittelt das ROM 102 über die Ansteuerleitung 114 einen Ansteuerimpuls an den Multiplexer 108. Der Multiplexer 108 holt daraufhin über die Datenleitung 109 einen der drei Schüssel KEY 3, KEY 2, KEY 1 aus dem FLASH-Speicher 104 und übermittelt diesen an die Verschlüsselungsbaugruppe 107. Daraufhin wird entweder der in der Verschlüsselungsbaugruppe 107 verwendete Schlüssel ausgetauscht oder je nach Wertigkeit des auf der Ansteuerleitung 116 anliegenden Signals eine Umschaltung zwischen einem in der Verschlüsselungsbaugruppe 107 angewendeten Verschlüsselungsverfahren bewirkt. Wird eine bestimmte Betriebszeit der Datenverarbeitungsschaltung überschritten, ohne daß der Multiplexer 108 durch das ROM 102 aktiviert wird, tritt der Timer 111 in Aktion. Durch die Betätigung des Timers 111 wird dem Multiplexer 108 über die Datenleitung 110 eine Zufallszahl aus dem Zufallsgenerator 113 übermittelt. Der Multiplexer 108 übermittelt dann die Zufallszahl an die Verschlüsselungsbaugruppe 107.

Die Daten in den Datenspeichern 102, 103, 104 und 105 sind verschlüsselt abgelegt. Daher werden die Daten auf dem Datenbus 106 verschlüsselt zur CPU 101 transportiert, wo sie von der Verschlüsselungsbaugruppe 107 wieder entschlüsselt werden. Erst danach stehen die Daten unverschlüsselt zur Verarbeitung in der CPU bereit.

Figur 2 zeigt eine Variante der Datenverarbeitungsschaltung aus Figur 1, die ebenfalls eine CPU 101 als Betriebsbaugruppe sowie mehrere Datenspeicher aufweist. Im Einzelnen sind dies ein ROM 102, ein EEPROM 103, ein FLASH-Speicher 104 sowie ein

RAM 105. Die Datenspeicher 102, 103, 104, 105 und die CPU 101 sind über einen Datenbus 106 miteinander verbunden.

In der CPU 101 ist eine Verschlüsselungsbaugruppe 107 vorgesehen, die den Datenverkehr zwischen CPU 1 und den Datenspeichern 102, 103, 104 sowie 105 verschlüsselt bzw. entschlüsselt.

Die Datenverarbeitungsschaltung aus Figur 2 hat im Gegensatz zu derjenigen aus Figur 1 keinen Multiplexer zur Versorgung der Verschlüsselungsbaugruppe 107 mit einem neuen Schlüssel. Statt dessen ist die Datenverarbeitungsschaltung aus Figur 2 über eine Ansteuerleitung 122 mit einer Umsetzungsbaugruppe 120 verbunden, die ihrerseits mit einem Adressbus 121 der CPU 101 in Verbindung steht. Zu der Umsetzungsbaugruppe 120 führt eine weitere Ansteuerleitung 123, mit der eine bestimmte Umsetzung aus einer Auswahl verschiedener in der Umsetzungsbaugruppe 120 gespeicherter Umsetzungen von "Adresse" auf "Schlüssel" auswählbar ist. Durch die Umsetzungsbaugruppe 120 wird dadurch ein Schlüssel aus einer in der CPU 101 anliegenden Adresse abgeleitet.

Im Betrieb verhält sich die elektronische Datenverarbeitungsschaltung aus Figur 2 im wesentlichen wie diejenige aus Figur 1. Beim Programmstart (RESET) wird auf ein Signal auf der Ansteuerleitung 123 ein Start-Schlüssel in der Verschlüsselungsbaugruppe 107 eingestellt. Daraufhin wird jeglicher Datenverkehr zwischen Datenbus 106 und CPU 101 in der Verschlüsselungsbaugruppe 107 verschlüsselt bzw. entschlüsselt, wobei bei jedem Durchgang von Daten durch die Verschlüsselungsbaugruppe 107 eine entsprechende Operation entsprechend der Datenflußrichtung ausgeführt wird. Bei jeder Aktivierung der Ansteuerleitung 123 leitet die Umsetzungsbaugruppe 120 auf der Basis einer neuen Umsetzung einen Schlüssel aus einer in der CPU 101 anliegenden Adresse ab.

Die Daten in den Datenspeichern 102, 103, 104 und 105 sind stets verschlüsselt abgelegt. Daher werden die Daten auf dem Datenbus 106 verschlüsselt zur CPU 101 transportiert, wo sie von der Verschlüsselungsbaugruppe 107 wieder entschlüsselt werden. Erst danach stehen die Daten unverschlüsselt zur Verarbeitung in der CPU bereit.

Die erfindungsgemäße Datenverarbeitungsschaltung aus Figur 3 hat eine CPU 1 als Betriebsbaugruppe sowie mehrere Datenspeicher. Im Einzelnen sind dies ein ROM 2, ein EEPROM 3, ein FLASH-Speicher 4 sowie ein RAM 5. Die Datenspeicher 2, 3, 4, 5 und die CPU 1 sind über einen in dieser Ansicht nicht dargestellten Datenbus miteinander verbunden. Anstelle des Datenbus sind in dieser Ansicht einzelne Datenleitungen 6, 7, 8, 9, 10, 11, 12, 13, 14 und 15 vorgesehen, über die die CPU 1 Daten mit den Datenspeichern 2, 3, 4, 5 austauscht. Zwischen der CPU 1 und dem ROM 2, dem EEPROM 3, dem FLASH 4 und dem RAM 5 ist noch je ein Latch-Zwischenspeicher 16, 17, 18, 19 angeordnet.

Im Bereich zwischen dem ROM 2 und dem Latch 16, im Bereich zwischen dem Latch 17 und der CPU 1, im Bereich zwischen den Latches 18, 19 und der CPU 1 sowie in der CPU 1 selbst sind Verschlüsselungsbaugruppen 20, 21, 22 und 35 vorgesehen, die den Datenverkehr auf den ihnen zugeordneten Datenleitungen verschlüsseln bzw. entschlüsseln. Hier sei noch einmal darauf hingewiesen, daß die derartigen Einrichtungen nachfolgend mit "Verschlüsselungsbaugruppe" bezeichnet werden, obwohl sie ausdrücklich nicht auf Einrichtungen beschränkt sind, die lediglich eine Verschlüsselung ausführen. Gemäß dem Grundgedanken der Erfindung sind mit dieser Bezeichnung auch Einrichtungen gemeint, die sowohl eine Verschlüsselung als auch eine Entschlüsselung bzw. nur eine dieser beiden Operationen ausführen. Die Ver- bzw. Entschlüsselung kann dabei durch eine geeignete Verzögerung, durch ein Vertauschen von einzelnen Bitleitungen der Datenleitungen oder durch ein

Verändern der Wertigkeit einzelner Datenbits erfolgen. Auch eine Software-Verschlüsselung kann ausgeführt werden.

Die Verschlüsselungsbaugruppen 20, 21, 22 und 35 sind so ausgebildet, daß der Datenverkehr auf den ihnen zugeordneten Datenleitungen jeweils nur teilweise verschlüsselt bzw. entschlüsselt wird. Eine vollständige Verschlüsselung bzw. Entschlüsselung ergibt sich erst bei einem Zusammenwirken je einer der Verschlüsselungsbaugruppen 20, 21, 22 mit der Verschlüsselungsbaugruppe 35.

Weiterhin hat die erfindungsgemäße Datenverarbeitungsschaltung einen Multiplexer 23, der über eine Datenleitung 24 mit dem FLASH-Speicher 4 in Verbindung steht. Der Multiplexer 23 steht über eine Datenleitung 25 mit einem Timer 26 in Verbindung, dem über eine Datenleitung 27 von einem Zufallszahlgenerator 28 eine Zufallszahl zuführbar ist. Der Multiplexer 23 weist auch eine Ansteuerleitung 29 auf, über die er mit dem ROM 2 in Verbindung steht.

Der Ausgang des Multiplexers 23 steht über Ansteuerleitungen 30, 31, 32, 33, 34 mit den Verschlüsselungsbaugruppen 20, 21, 22, 35 in Verbindung, wobei die Verschlüsselungsbaugruppen 20, 21, 22, 35 auf ein Ausgangssignal des Multiplexers 23 hin mit einem neuen Schlüssel versorgt werden.

Im Betrieb verhält sich die erfindungsgemäße elektronische Datenverarbeitungsschaltung wie folgt. Bei jeder Ausführung des Befehls "CLR C" übermittelt das ROM 2 über die Ansteuerleitung 29 einen Ansteuerimpuls an den Multiplexer 23. Der Multiplexer 23 holt daraufhin über die Datenleitung 24 einen der drei Schlüssel KEY 3, KEY 2, KEY 1 aus dem FLASH-Speicher 4 und übermittelt diesen an die Verschlüsselungsbaugruppen 20, 21, 22 und 35. Wird eine vorbestimmte Betriebszeit der Datenverarbeitungsschaltung überschritten, ohne daß der Multiplexer 23 durch das ROM 2 aktiviert wird, dann tritt der Timer 26 in Aktion. Durch die Betätigung des Timers 26 wird

dem Multiplexer 23 über die Datenleitung 25 eine Zufallszahl aus dem Zufallsgenerator 28 übermittelt. Der Multiplexer 23 übermittelt dann die Zufallszahl an die Verschlüsselungsbaugruppen 20, 21, 22, 35.

Die Daten im ROM 2 sind verschlüsselt abgelegt und sie werden beim Auslesen in den Latch 16 durch die Verschlüsselungsvorrichtung 20 nur teilweise entschlüsselt. Daher werden die Daten aus dem ROM 2 auf der Datenleitung 8 noch teilweise verschlüsselt bis zur CPU 1 transportiert, wo sie von der Verschlüsselungsbaugruppe 35 vollständig entschlüsselt werden. Erst danach stehen die Daten unverschlüsselt zur Verarbeitung in der CPU 1 bereit.

Die verschlüsselt im EEPROM 3 vorgesehenen Daten werden verschlüsselt über die Datenleitung 9 an den Latch 17 übermittelt und von dort an die Verschlüsselungsbaugruppe 21 weitergeleitet, wo sie teilweise entschlüsselt werden. Von dort gelangen die noch teilweise verschlüsselten Daten über die Datenleitung 11 zur CPU 1, wo sie von der Verschlüsselungsbaugruppe 35 vollständig entschlüsselt werden und danach zur Verarbeitung bereitstehen.

Daten für den FLASH-Speicher 4 und für das RAM 5 werden zunächst jeweils teilweise durch die Verschlüsselungsbaugruppe 35 und durch die Verschlüsselungsbaugruppe 22 verschlüsselt, bevor sie vollständig verschlüsselt im FLASH-Speicher 4 oder im RAM 5 abgespeichert werden. Dazu werden die in der Verschlüsselungsbaugruppe 35 der CPU 1 teilweise verschlüsselten Daten über die Datenleitung 11 an die Verschlüsselungsbaugruppe 22 übermittelt, wo sie vollständig verschlüsselt werden, bevor sie über die Datenleitungen 13 bzw. 14 an die dem FLASH-Speicher 4 und dem RAM 5 zugeordneten Latches 18, 19 übergeben werden. Von den Latches 18, 19 gelangen die verschlüsselten Daten über Datenleitungen 12, 15 zum FLASH-Speicher 4 bzw. RAM 5.

Beim Auslesen der Daten aus dem FLASH-Speicher 4 und aus dem RAM 5 werden diese zunächst jeweils teilweise durch die Verschlüsselungsbaugruppe 22 und durch die Verschlüsselungsbaugruppe 35 entschlüsselt, bevor sie vollständig entschlüsselt in der CPU 1 zur Verarbeitung bereitstehen.

# Elektronische Datenverarbeitungsschaltung

## Patentansprüche

1. Elektronische Datenverarbeitungsschaltung mit einer Betriebsbaugruppe wie einem Mikroprozessor, mit wenigstens einem Datenspeicher und mit einem sich zwischen Datenspeicher und Betriebsbaugruppe erstreckendem Datenbus, dadurch gekennzeichnet, daß im Bereich zwischen Datenspeicher (2, 3, 4, 5, 102, 103, 104, 105) und Datenbus (106) und/oder im Bereich zwischen Betriebsbaugruppe (1, 101) und Datenbus (106) wenigstens eine Verschlüsselungsbaugruppe (20, 21, 22, 35, 107) vorgesehen ist, wobei die Verschlüsselungsbaugruppe (20, 21, 22, 35, 107) so ausgebildet ist, daß Datenverkehr zwischen Betriebsbaugruppe (1, 101) und Datenbus (106) bzw. zwischen Datenspeicher (2, 3, 4, 5, 102, 103, 104, 105) und Datenbus (106) verschlüsselbar und/oder entschlüsselbar ist.

2. Elektronische Datenverarbeitungsschaltung nach Anspruch 1, dadurchgekennzeichnet, daß die Verschlüsselungsbaugruppe (20, 21, 22, 35, 107) so ausgebildet ist, daß der Datenverkehr mittels eines Verschlüsselungs-Algorithmus verschlüsselbar ist.

3. Elektronische Datenverarbeitungsschaltung nach Anspruch 1 oder Anspruch 2, dadurch gekennzeichnet, daß die Verschlüsselungsbaugruppe (20, 21, 22, 35, 107) so ausgebildet ist, daß der Datenverkehr mittels Hardware-Verschlüsselung verschlüsselbar ist.

4. Elektronische Datenverarbeitungsschaltung nach Anspruch 3, dadurch gekennzeichnet, daß die Verschlüsselungsbaugruppe (20, 21, 22, 35, 107) so ausgebildet ist, daß die Wertigkeit einzelner Bits des Datenverkehrs selektiv änderbar ist.

5. Elektronische Datenverarbeitungsschaltung nach Anspruch 4, dadurch gekennzeichnet, daß die Verschlüsselungsbaugruppe wenigstens ein EXOR-Glied aufweist.

6. Elektronische Datenverarbeitungsschaltung nach einem der Ansprüche 3 bis 5, dadurch gekennzeichnet, daß die Verschlüsselungsbaugruppe (20, 21, 22, 35, 107) so ausgebildet ist, daß die Anschlußreihenfolge von Datenleitungen des Datenbus selektiv änderbar ist.

7. Elektronische Datenverarbeitungsschaltung nach einem der Ansprüche 3 bis 6, dadurch gekennzeichnet, daß die Verschlüsselungsbaugruppe (20, 21, 22, 35, 107) so ausgebildet ist, daß der Datenverkehr wenigstens teilweise selektiv verzögerbar ist.

8. Elektronische Datenverarbeitungsschaltung nach einem der Ansprüche 3 bis 7, dadurch gekennzeichnet, daß die Verschlüsselungsbaugruppe (20, 21, 22, 35, 107) wenigstens einen Eingang zur Eingabe wenigstens eines Schlüssels aufweist.

9. Elektronische Datenverarbeitungsschaltung nach Anspruch 8, dadurch gekennzeichnet, daß der bzw. die Schlüssel in einer Flash-Zelle der Datenverarbeitungsschaltung abgelegt ist bzw. sind.

10. Elektronische Datenverarbeitungsschaltung nach Anspruch 8 oder 9, dadurch gekennzeichnet, daß der Schlüssel in einer vergrabenen Struktur eines integrierten Bausteins zur Aufnahme der Datenverarbeitungsschaltung abgelegt ist.

11. Elektronische Datenverarbeitungsschaltung nach Anspruch 8 oder 9, dadurch gekennzeichnet, daß eine Sensorik zum Abtasten von Manipulationen des Orts, an dem der Schlüssel abgelegt ist, aufweist.

12. Elektronische Datenverarbeitungsschaltung nach einem der Ansprüche 8 bis 11, dadurch gekennzeichnet, daß die Datenverarbeitungsschaltung so ausgebildet ist, daß bei Ausführung vorbestimmter Operationen durch die Betriebsbaugruppe ein Schlüssel in die Verschlüsselungsbaugruppe (20, 21, 22, 35, 107) eingebbar ist.

13. Elektronische Datenverarbeitungsschaltung nach einem der Ansprüche 8 bis 12, dadurch gekennzeichnet, daß ein Zufallsgenerator (28) vorgesehen ist, mit dem ein Schlüssel zufällig auswählbar ist.

14. Elektronische Datenverarbeitungsschaltung nach einem der Ansprüche 8 bis 12, dadurch gekennzeichnet, daß eine Einrichtung (120) zum Ableiten eines Schlüssels aus einer in der Betriebsbaugruppe (101) verwendeten Adresse vorgesehen ist.

15. Elektronische Datenverarbeitungsschaltung nach einem der Ansprüche 8 bis 13, dadurch gekennzeichnet, daß eine Zeitmessvorrichtung (26) vorgesehen ist, durch die ein Wechsel des Schlüssels einleitbar ist.

16. Elektronische Datenverarbeitungsschaltung nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß im Bereich mindestens einer die Betriebsbaugruppe (1) und wenigstens einen Datenspeicher (2, 3, 4, 5) verbindenden Datenleitung (7, 8, 34, 11) des Datenbus wenigstens zwei Verschlüsselungsbaugruppen (18, 19, 20, 21, 35) vorgesehen sind, wobei die Verschlüsselungsbaugruppen (18, 19, 20, 21, 35) so ausgebildet sind, daß eine vollständige Verschlüsselung bzw. Entschlüsselung durch das Zusammenwirken der Verschlüsselungsbaugruppen (18, 19, 20, 21, 35) ausführbar ist.

17. Elektronische Datenverarbeitungsschaltung nach Anspruch 16, dadurch gekennzeichnet, daß die Verschlüsselungsbaugruppen (18, 19, 20, 21, 35) an verschiedenen Orten der elektronischen Datenverarbeitungsschaltung angeordnet sind.

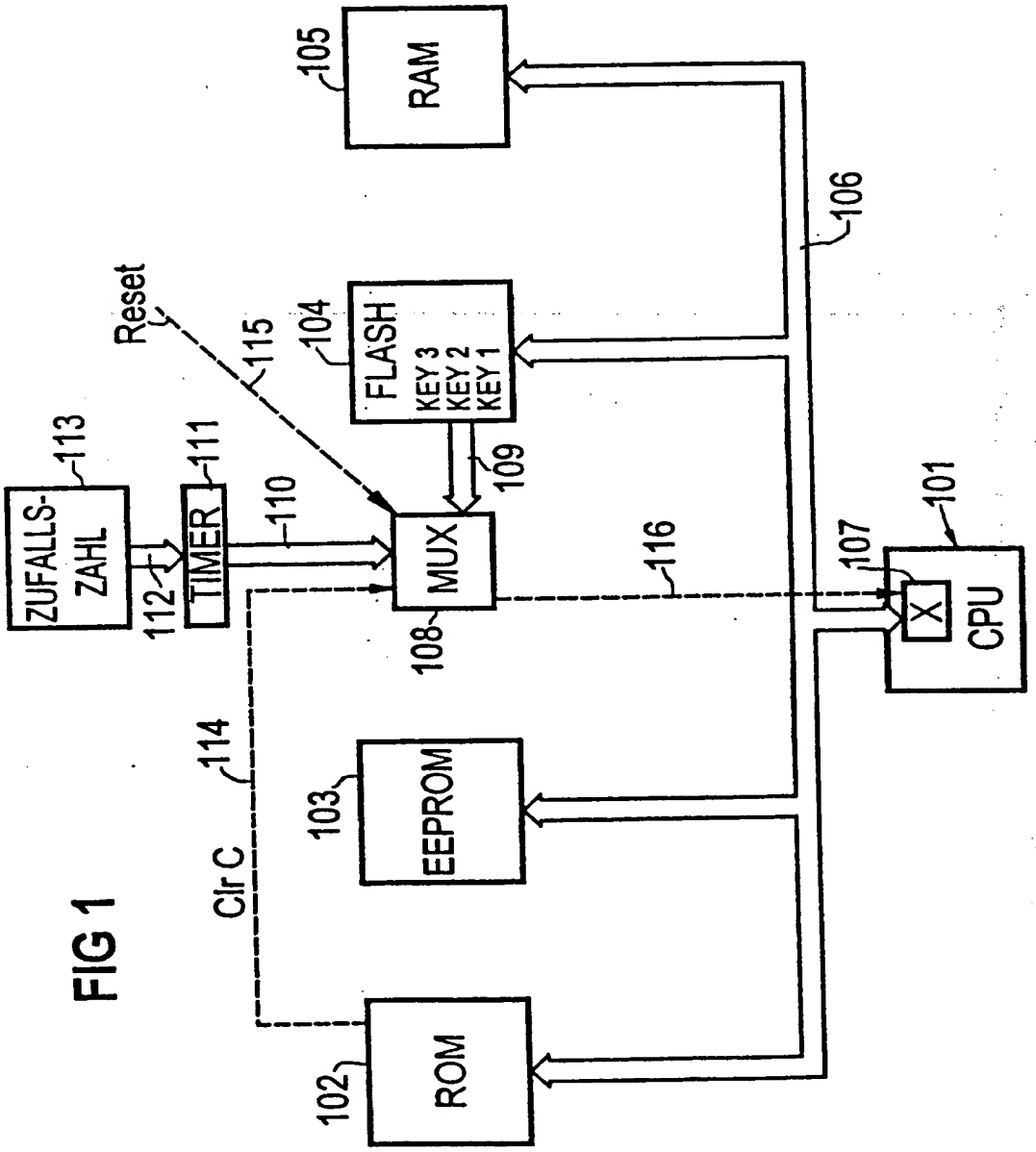

RAM
105
106
FLASH
KEY 3
KEY 2
KEY 1
104
Reset
115
109
ZUFALLS-
ZAHL
113
TIMER
111
110
MUX
112
108
116
107
101
CPU
X
114
EEPROM
103
Clr C
ROM
102

FIG 1

FIG 2

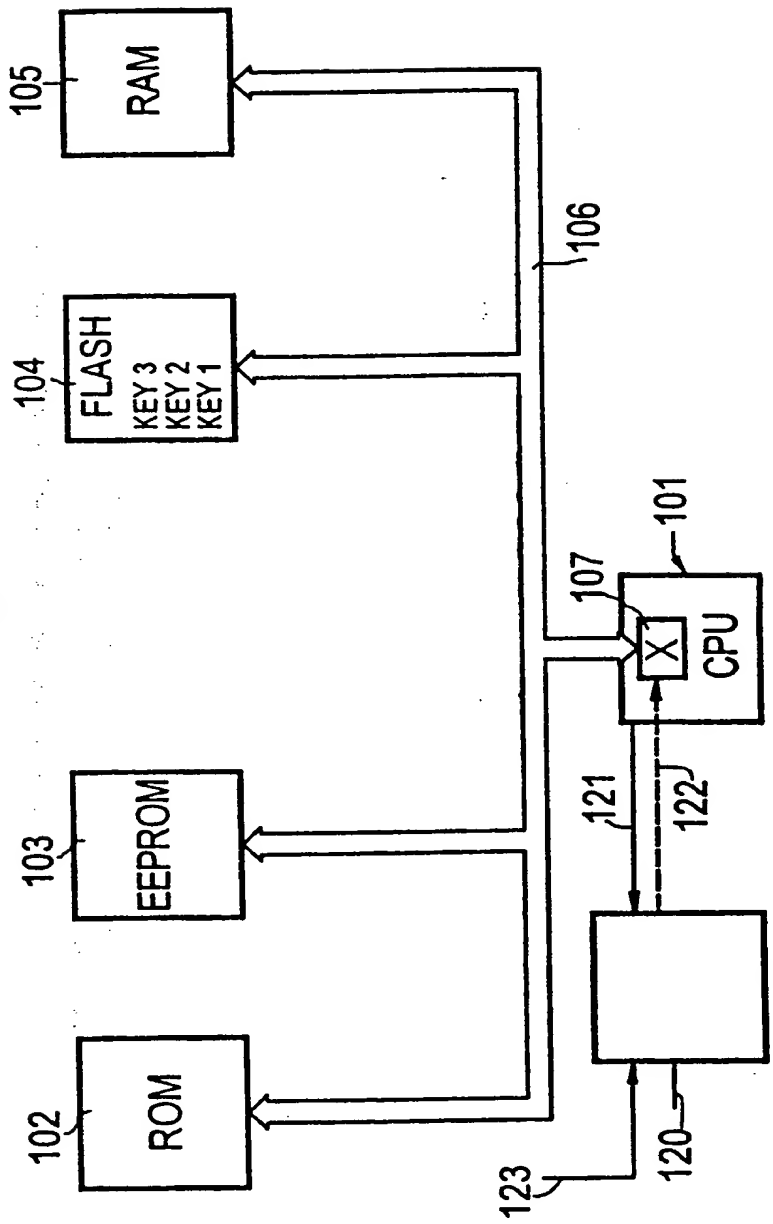
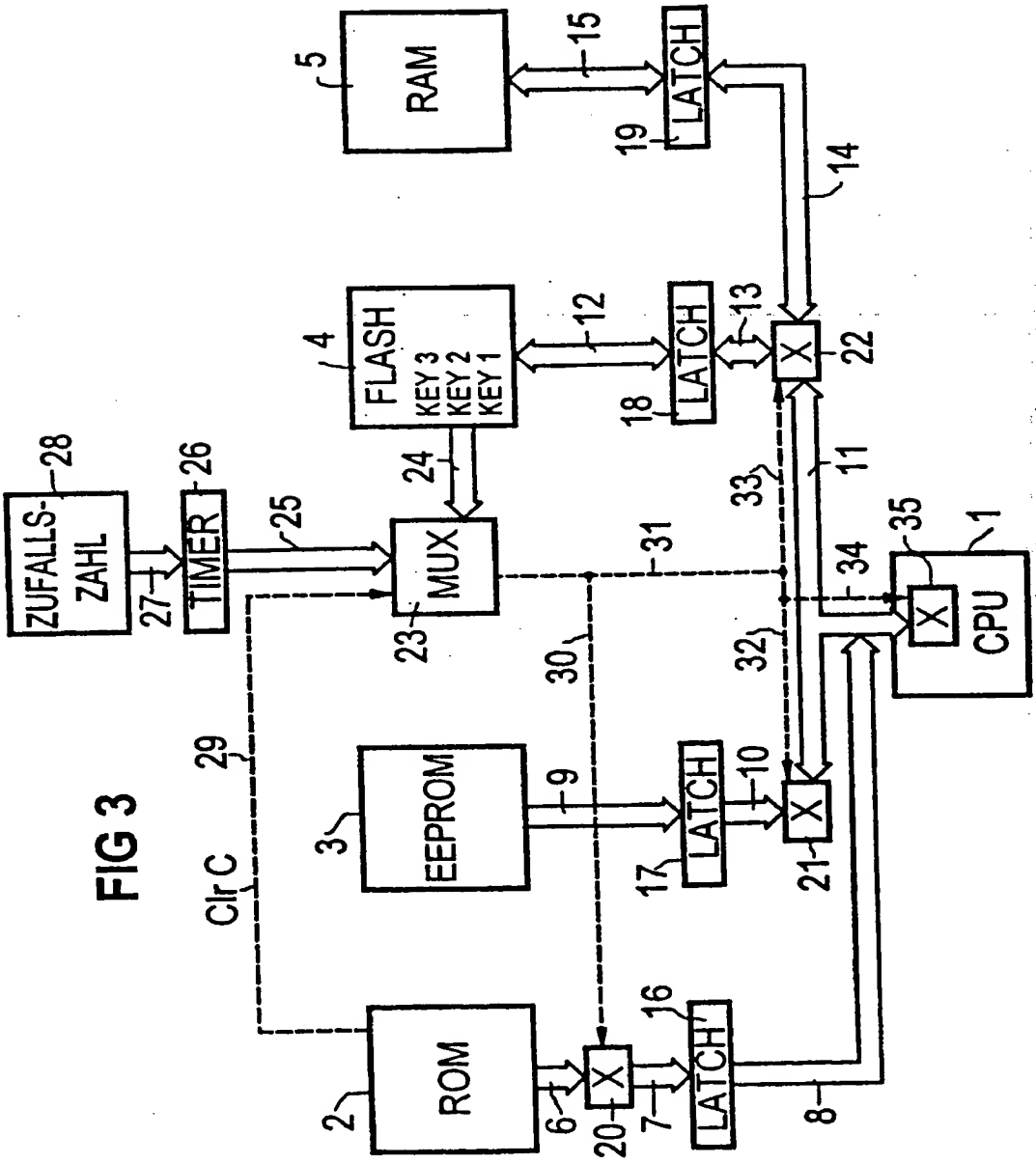

105
RAM
106
104
FLASH
KEY 3
KEY 2
KEY 1
101
107
X1
CPU
121
122
103
EEPROM
102
ROM
123
120

FIG 3


RAM
5
15
LATCH
19
14
FLASH
KEY 3
KEY 2
KEY 1
4
12
LATCH
18
13
X
22
ZUFALLS-
ZAHL
28
TIMER
26
27
25
MUX
24
23
31
33
11
35
1
34
X
CPU
32
30
29
EEPROM
3
9
LATCH
17
10
X
21
ClrC
ROM
2
6
X
20
7
LATCH
16
8

# INTERNATIONAL SEARCH REPORT

Inter ɔnal Application No
PCT/DE 97/02070

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F12/14

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | EP 0 449 256 A (TOKYO SHIBAURA ELECTRIC CO ;TOSHIBA MICRO ELECTRONICS (JP)) 2 October 1991 see the whole document | 1,3-5 |
| Y | --- | 16,17 |
| Y | GB 2 099 616 A (JPM AUTOMATIC MACHINES LTD) 8 December 1982 see the whole document | 16,17 |
| | --- | |
| X | "SECTION 1: INTRODUCTION" DATA BOOK SOFT MICROCONTROLLER, 6 October 1993, pages 1-3, 7, 8, 73, 77-80, 82, 152-156, 229, 290-292, XP002053731 | 1,2 |
| Y | --- | 3-6,8-15 |
| | -/-- | |

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 28 January 1998 | 18/02/1998 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | Powell, D |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/DE 97/02070

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 5 386 469 A (YEARSLEY GYLE ET AL) 31 January 1995<br>see abstract; figure 1 | 3-6,8-15 |
| A | US 4 598 170 A (PIOSENKA GERALD V ET AL)<br>1 July 1986<br>see the whole document | 6 |
| A | WO 95 16238 A (TELEQUIP CORP) 15 June 1995<br>see abstract; figure 2<br>see page 2, line 14 - line 27<br>see page 4, line 29 - page 5, line 7 | 9 |

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ional Application No
PCT/DE 97/02070

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| EP 0449256 A | 02-10-91 | JP 3276345 A | 06-12-91 |
| | | DE 69126557 D | 24-07-97 |
| | | DE 69126557 T | 13-11-97 |
| | | US 5214697 A | 25-05-93 |
| GB 2099616 A | 08-12-82 | NONE | |
| US 5386469 A | 31-01-95 | NONE | |
| US 4598170 A | 01-07-86 | NONE | |
| WO 9516238 A | 15-06-95 | AU 1265195 A | 27-06-95 |
| | | US 5623637 A | 22-04-97 |

# INTERNATIONALER RECHERCHENBERICHT

Inte onales Aktenzeichen
PCT/DE 97/02070

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06F12/14

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole )
IPK 6 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| X | EP 0 449 256 A (TOKYO SHIBAURA ELECTRIC CO ;TOSHIBA MICRO ELECTRONICS (JP)) 2.Oktober 1991<br>siehe das ganze Dokument | 1,3-5 |
| Y | --- | 16,17 |
| Y | GB 2 099 616 A (JPM AUTOMATIC MACHINES LTD) 8.Dezember 1982<br>siehe das ganze Dokument | 16,17 |
| | --- | |
| X | "SECTION 1: INTRODUCTION"<br>DATA BOOK SOFT MICROCONTROLLER,<br>6.Oktober 1993,<br>Seiten 1-3, 7, 8, 73, 77-80, 82, 152-156,<br>229, 290-292, XP002053731 | 1,2 |
| Y | --- | 3-6,8-15 |
| | -/-- | |

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

| Datum des Abschlusses der Internationalen Recherche | Absendedatum des internationalen Recherchenberichts |
|---|---|
| 28.Januar 1998 | 18/02/1998 |

| Name und Postanschrift der Internationalen Recherchenbehörde | Bevollmächtigter Bediensteter |
|---|---|
| Europäisches Patentamt, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | Powell, D |

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

# INTERNATIONALER RECHERCHENBERICHT

Inte. onales Aktenzeichen
PCT/DE 97/02070

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|---|---|---|
| Y | US 5 386 469 A (YEARSLEY GYLE ET AL)<br>31.Januar 1995<br>siehe Zusammenfassung; Abbildung 1 | 3-6,8-15 |
| A | US 4 598 170 A (PIOSENKA GERALD V ET AL)<br>1.Juli 1986<br>siehe das ganze Dokument | 6 |
| A | WO 95 16238 A (TELEQUIP CORP) 15.Juni 1995<br>siehe Zusammenfassung; Abbildung 2<br>siehe Seite 2, Zeile 14 - Zeile 27<br>siehe Seite 4, Zeile 29 - Seite 5, Zeile 7 | 9 |

1

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Inter. ..ales Aktenzeichen
PCT/DE 97/02070

| Im Recherchenbericht angeführtes Patentdokument | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | Datum der Veröffentlichung |
|---|---|---|---|
| EP 0449256 A | 02-10-91 | JP 3276345 A | 06-12-91 |
| | | DE 69126557 D | 24-07-97 |
| | | DE 69126557 T | 13-11-97 |
| | | US 5214697 A | 25-05-93 |
| GB 2099616 A | 08-12-82 | KEINE | |
| US 5386469 A | 31-01-95 | KEINE | |
| US 4598170 A | 01-07-86 | KEINE | |
| WO 9516238 A | 15-06-95 | AU 1265195 A | 27-06-95 |
| | | US 5623637 A | 22-04-97 |